

FIG. 1
(Prior Art)

FIG. 2
(Prior Art)

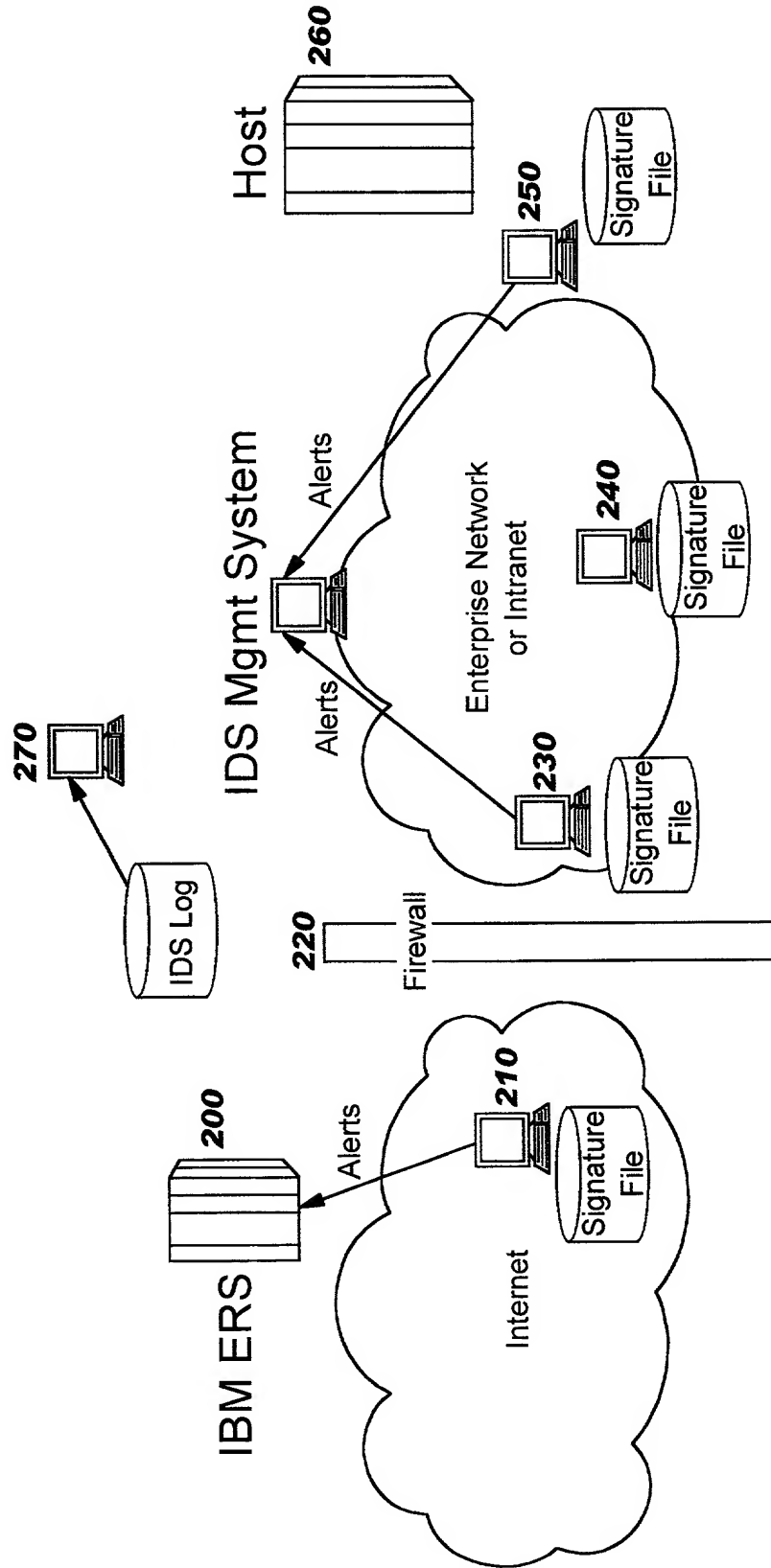


FIG. 3

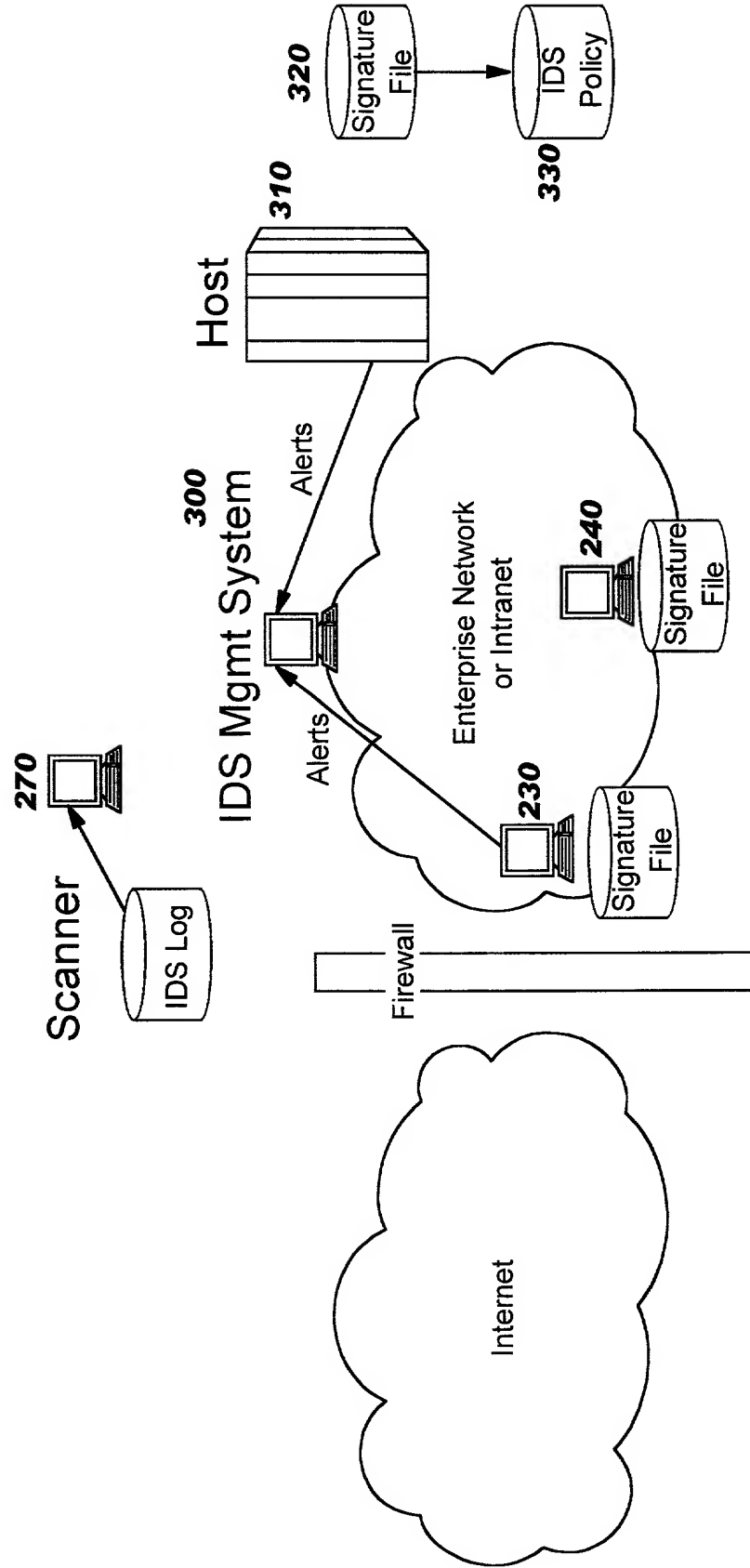


FIG. 4

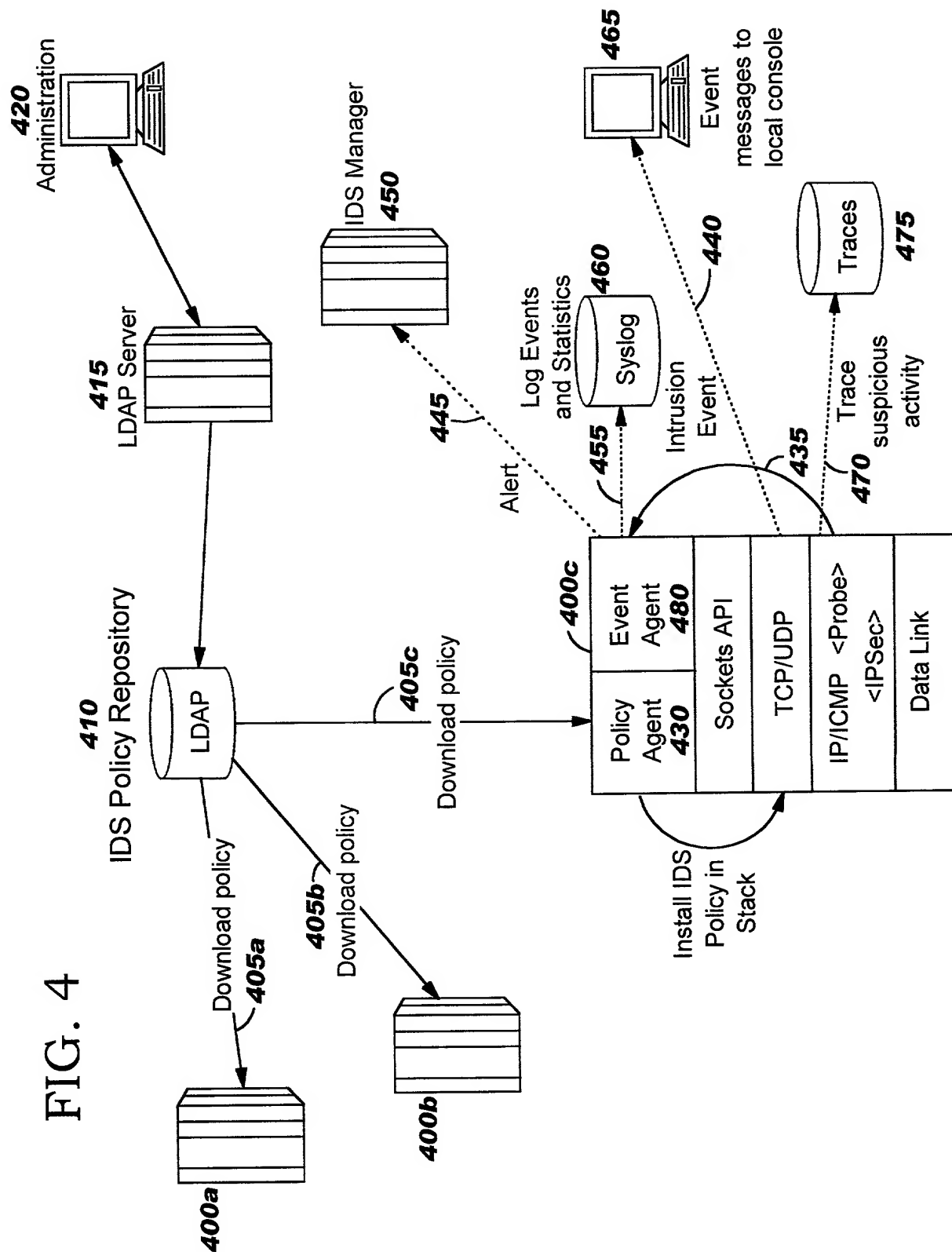


FIG. 6

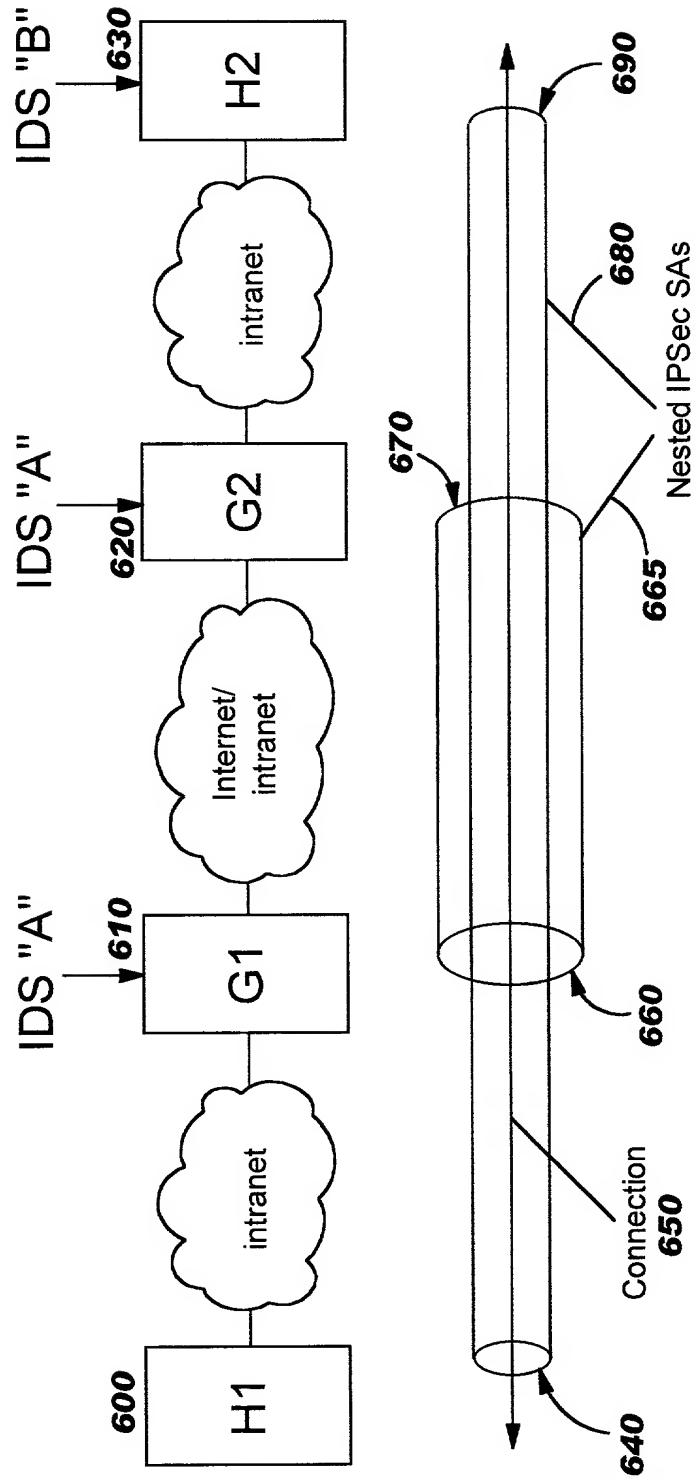


FIG. 7
(Prior Art)

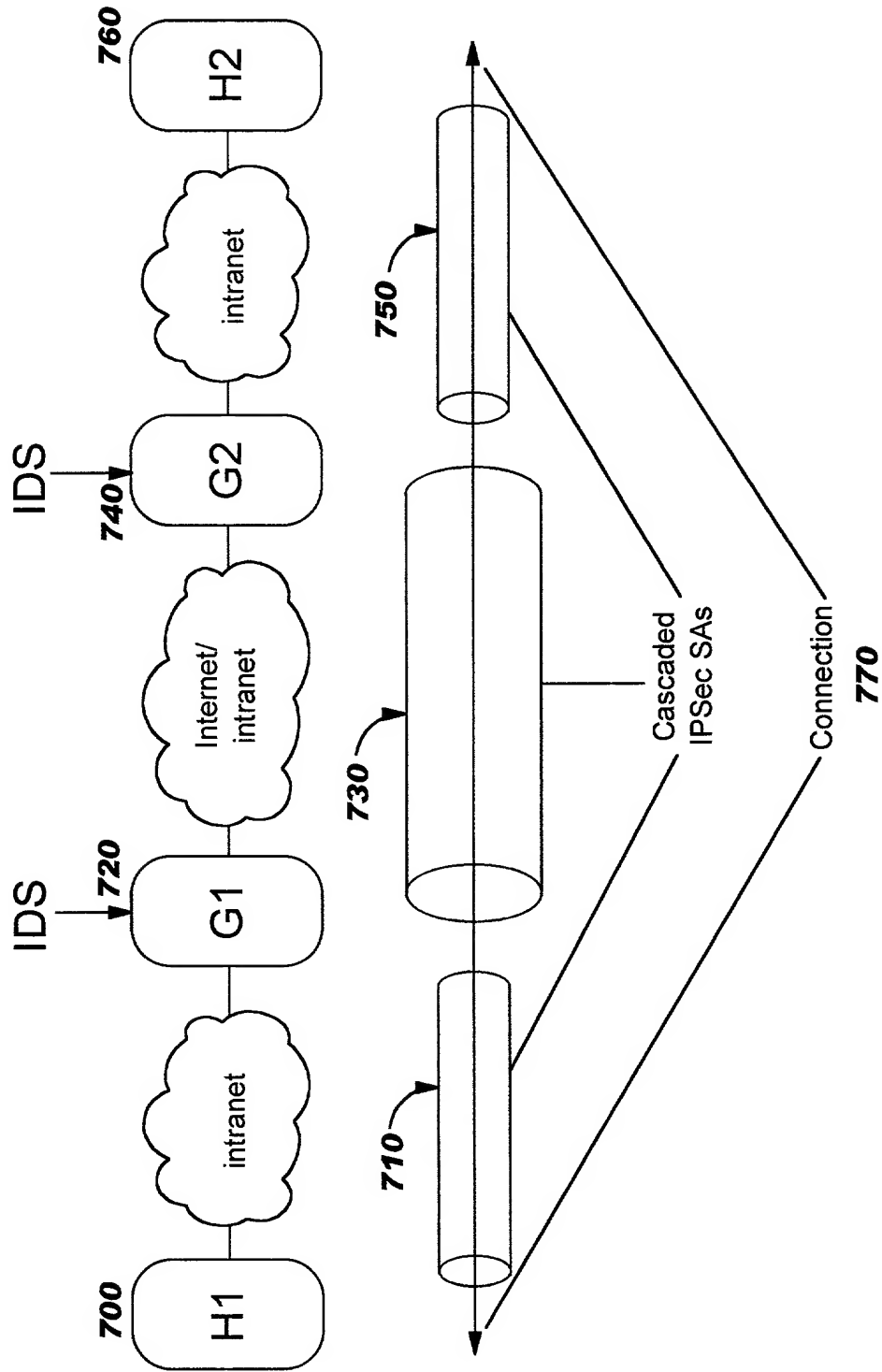
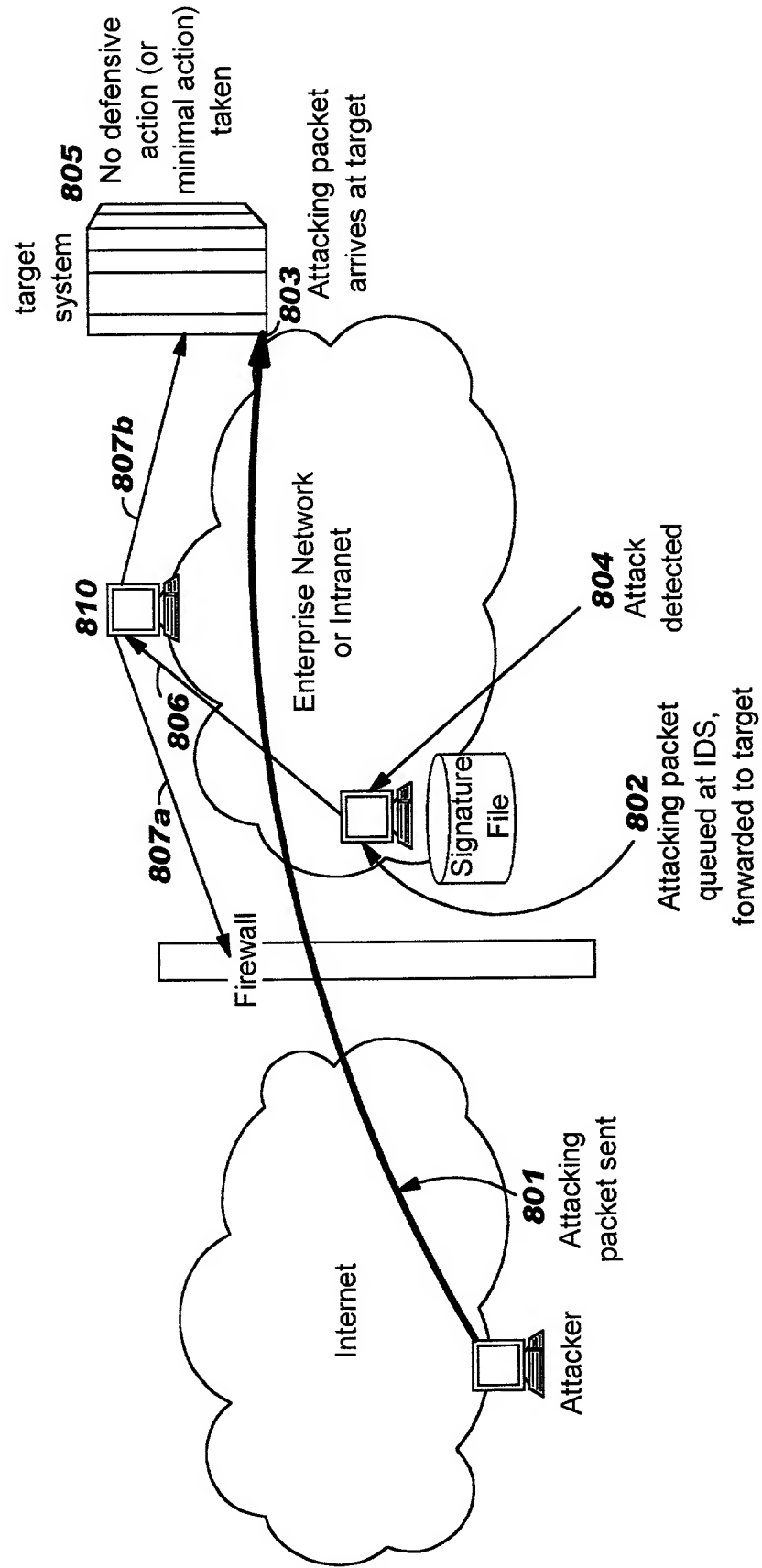


FIG. 8
(Prior Art)



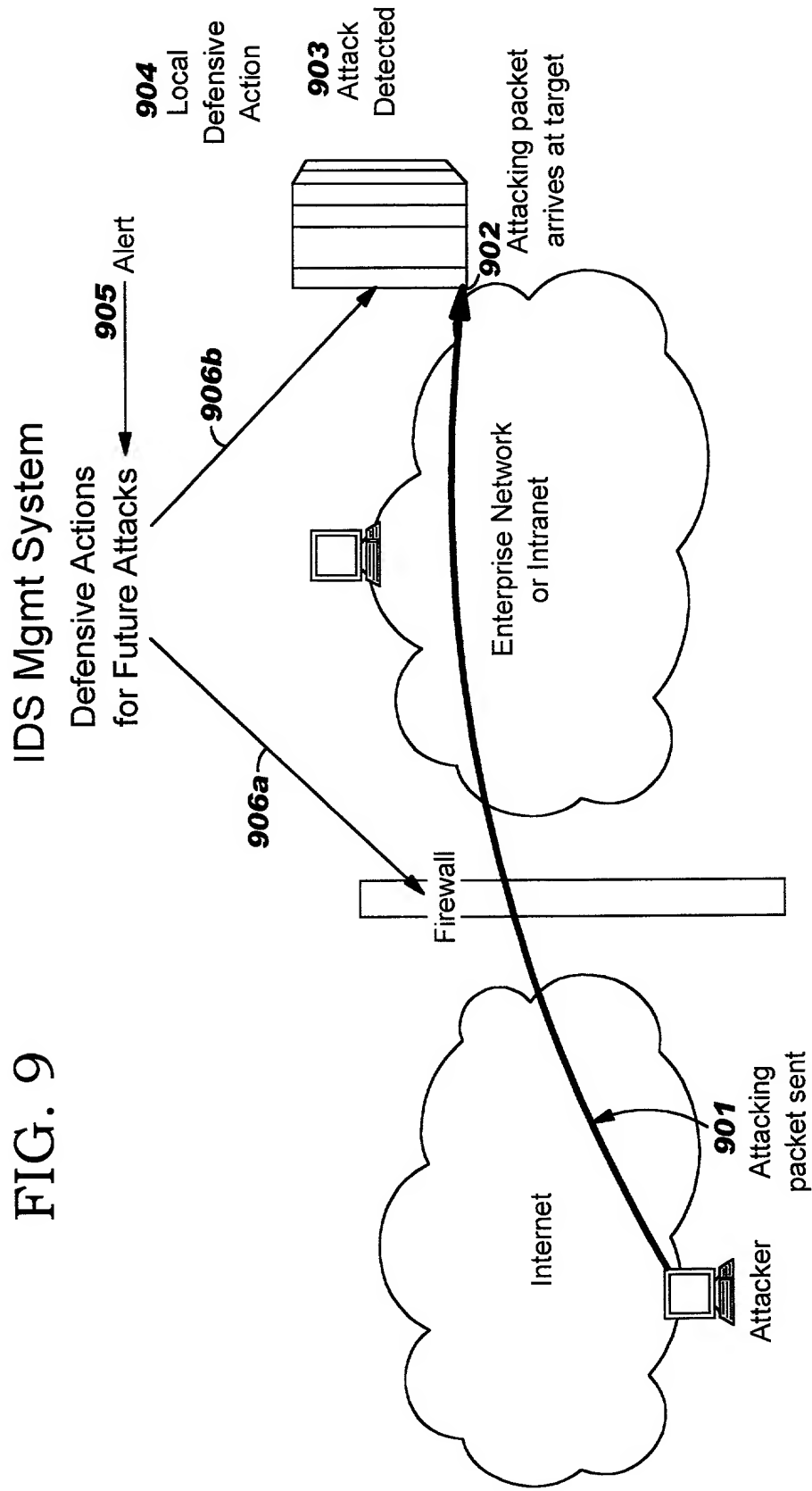


FIG. 10

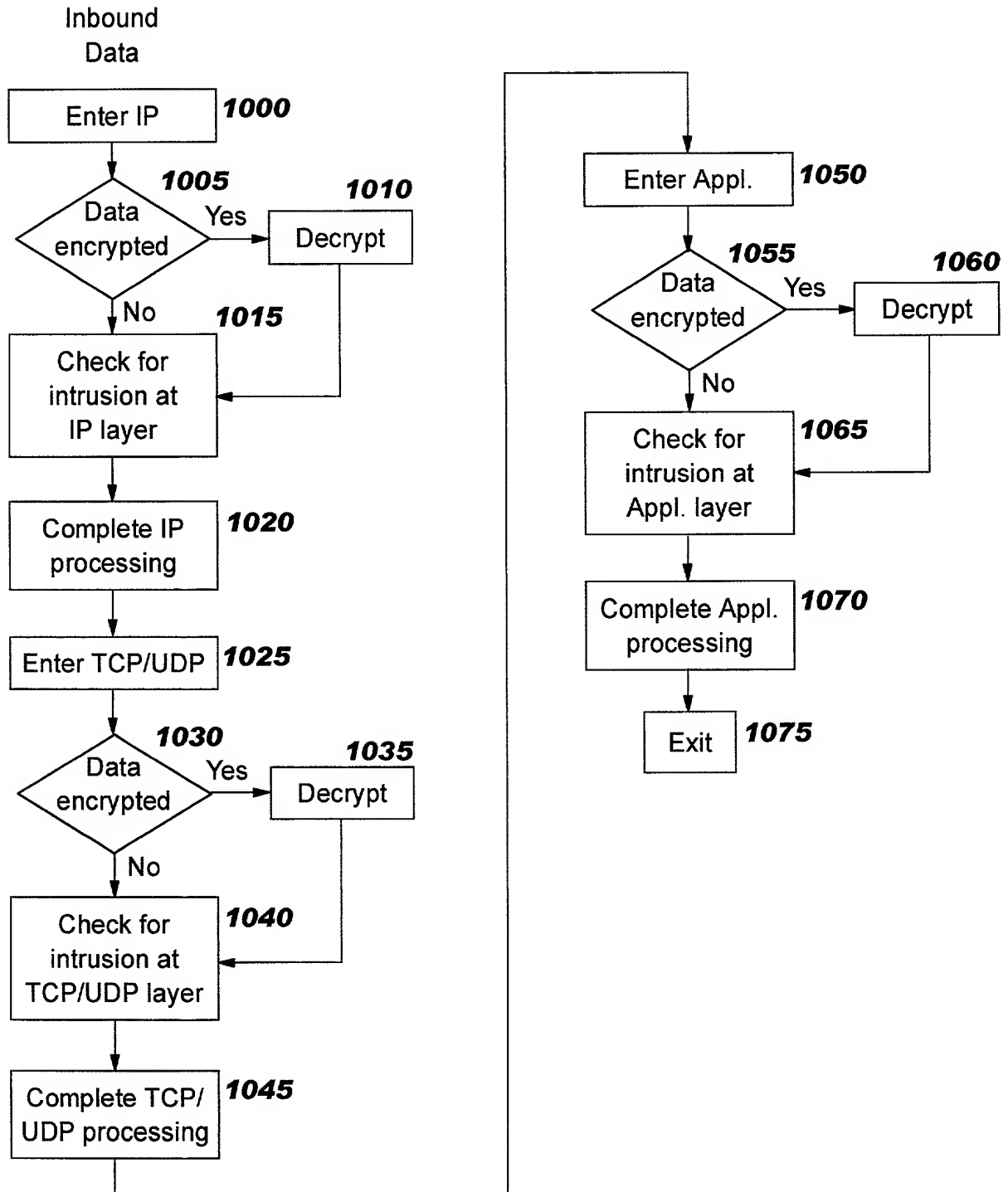


FIG. 11

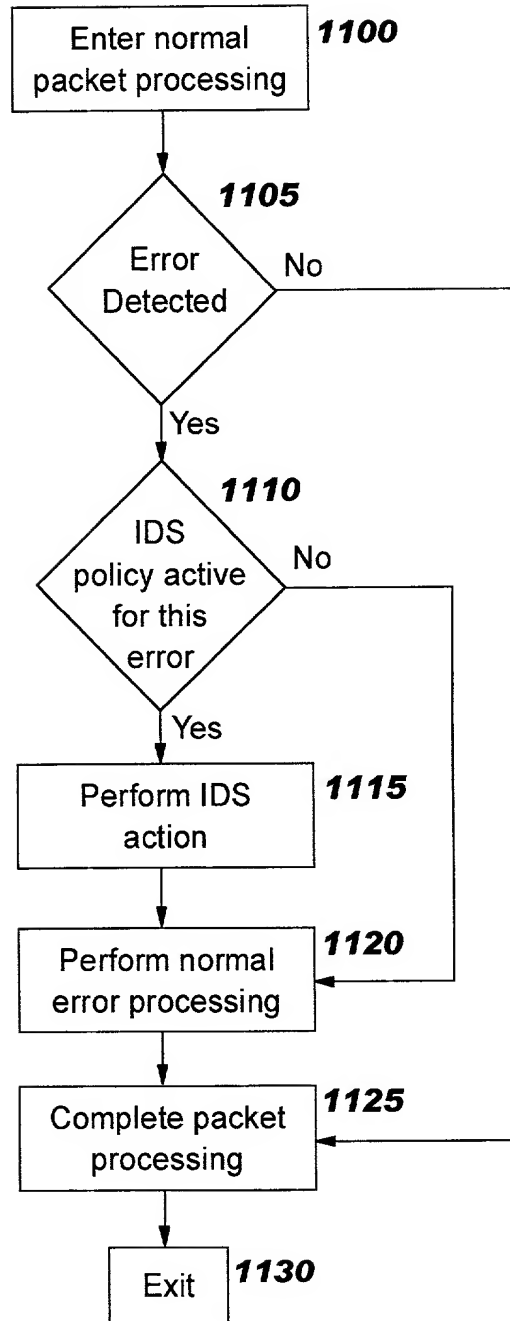
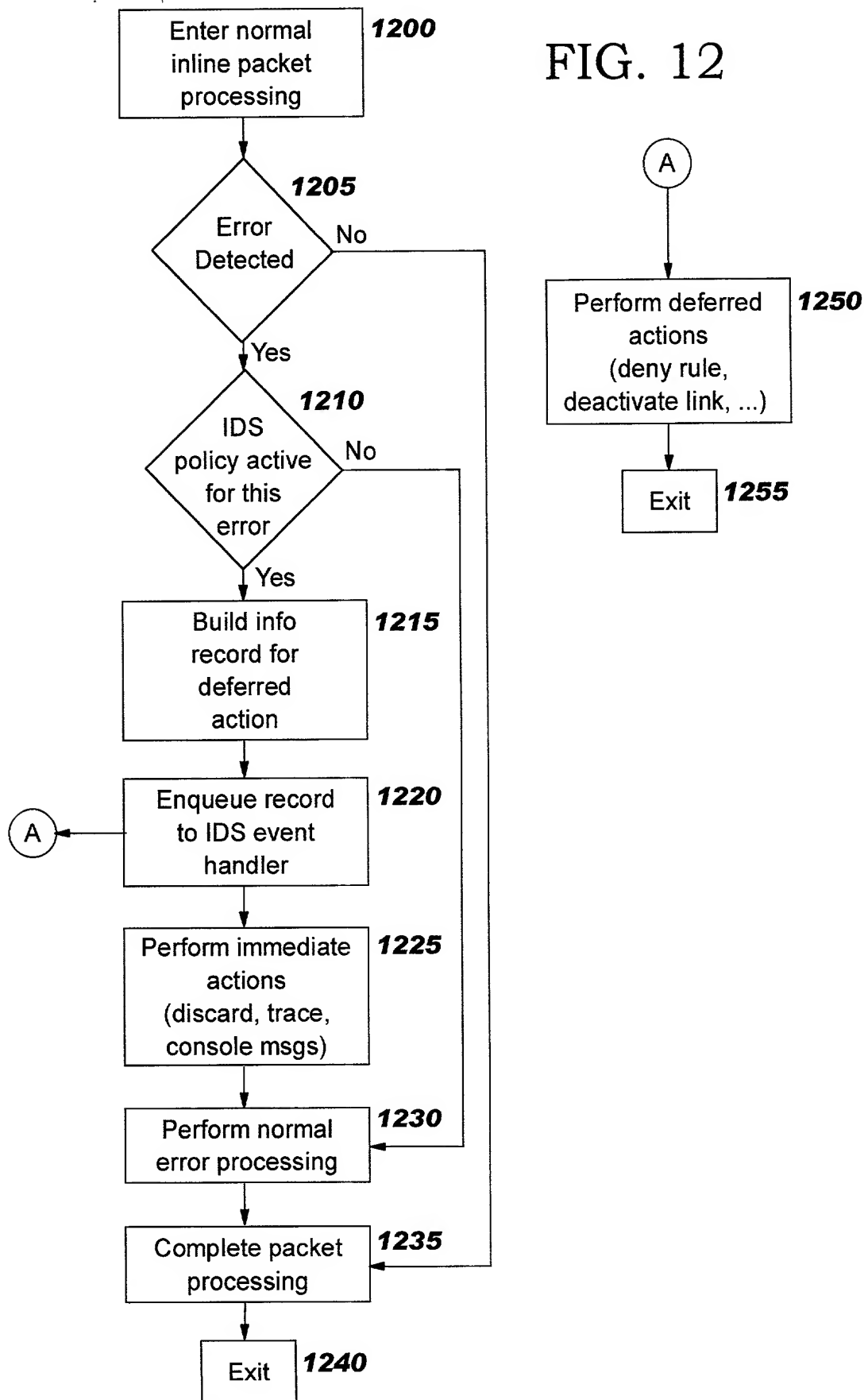


FIG. 12



```

graph TD
    1300{IDS policy active for this error or intrusion} -- Yes --> B1((B))
    1300 -- No --> 1305[Determine sensitivity level from policy]
    1305 --> 1310[Determine suspicion level of event]
    1310 --> 1315{Suspicion level = low}
    1315 -- Yes --> 1320{Sensitivity = high}
    1315 -- No --> 1325{Suspicion level = medium}
    1320 -- Yes --> 1345[Perform IDS action processing]
    1320 -- No --> B2((B))
    1325 -- Yes --> 1330{Sensitivity ≥ medium}
    1325 -- No --> 1335{Suspicion level = high}
    1330 -- Yes --> 1345
    1330 -- No --> B3((B))
    1335 -- Yes --> 1340{Sensitivity ≥ low}
    1335 -- No --> 1350[Exit]
    1340 -- Yes --> 1345
    1340 -- No --> 1350
    1345 --> 1350
    B4((B)) --> 1350
    1350[Exit]

```

FIG. 14

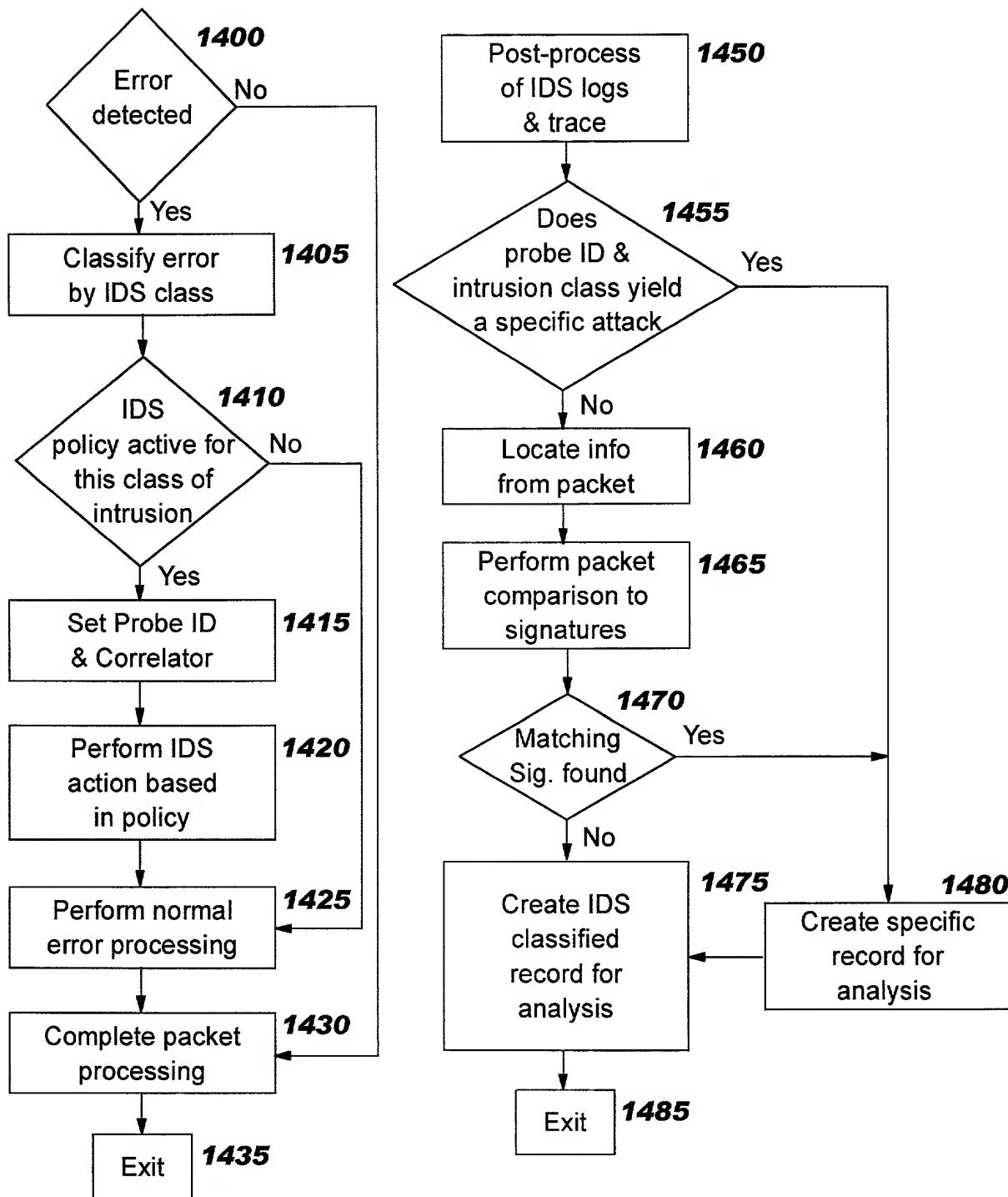


FIG. 15

1500

Sensitivity (from policy)	Low Suspicion Event (LS)	Medium Suspicion Event (MS)	High Suspicion Event (HS)
Low			Count
Medium		Count	Count
High	Count	Count	Count

1510 **1520** **1530**

FIG. 16

Basic Policy Objects

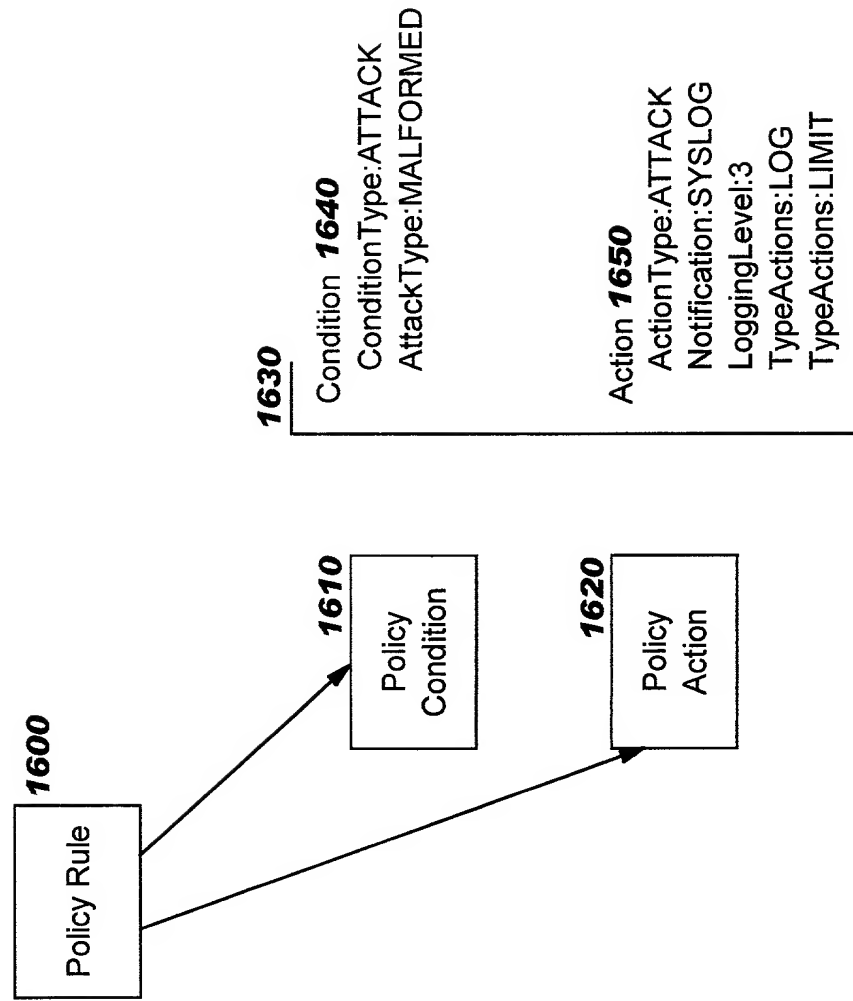


FIG. 17

1710 Socket State	1720 Event	1730 Event Classification
Any state	recv unexpected flags (SYN+FIN...)	high suspicion
RESERVED	recv any packet	high suspicion
Unbound, not RESERVED	recv any packet	medium suspicion - app may be temporarily down
Listen	recv SYN	classification deferred if syn queued.
Half open connection	recv ACK	low suspicion - connection handshake completed
Half open connection	recv RST	medium suspicion - scanner covering tracks?
Half open connection	final time-out (and not syn flood)	high suspicion - scanner abandoning handshake?
Any connected state	seq# out of window	low suspicion - perhaps duplicate packet
Any connected state	recv standalone SYN	low suspicion - perhaps peer reboot
Any connected state	final time-out	medium suspicion - peer abandoned connection

1700

1740

 Policy Sensitivity and Event
 Suspicion Levels for
 TCP Port Scan

1750

FIG. 18
IDS Policy Sensitivity and Event Suspicion Levels

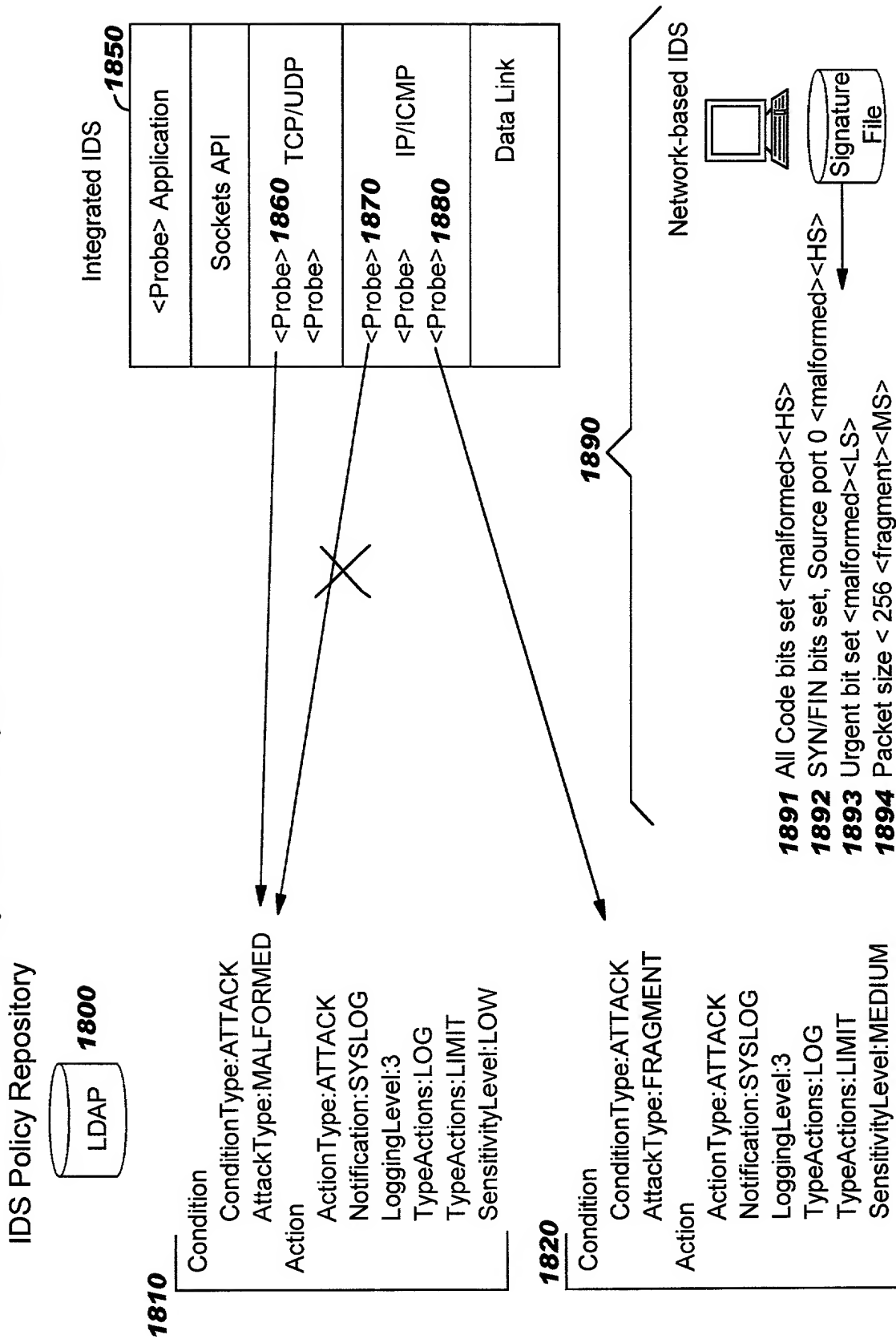


FIG. 19

Conditions and Actions - Relationship to specific attacks

